TAGUNGSBERICHTE

Erlanger Cybercrime Tag 2018: Darknet und Underground Economy

von Akad. Rat a.Z. Dr. Christian Rückert
und Wiss. Mit. Marlene Wüst

Der Tagungsbericht enthält sprachlich bereinigte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Dementsprechend ist auch der Fußnotenapparat auf ein notwendiges Minimum reduziert. Der Erlanger Cybercrime Tag 2018 wurde vom Bundesministerium des Innern, für Bau und Heimat gefördert.

Im Anschluss an die erfolgreiche Tagung zu virtuellen Kryptowährungen im Jahr 2017 fand am 21.2.2018 der zweite Erlanger Cybercrime Tag statt. Über 100 Besucher strömten in den reizvollen Wassersaal der Erlanger Orangerie; unter ihnen Vertreterinnen und Vertreter der Polizei- und Finanzbehörden, der Anwaltschaft, der Informatik und der Rechtswissenschaft sowie aus Wirtschaft und Industrie. Erfreulicherweise hatten auch zahlreiche Studierende den Weg zur Tagung gefunden. Thema der vom Bundesinnenministerium geförderten Konferenz war dieses Jahr das „Darknet" und die „Underground Economy". Die hohe gesellschaftliche und rechtspolitische Brisanz des Themas wird nicht zuletzt durch den aktuellen Koalitionsvertrag deutlich, welcher die Schaffung eines eigenen Straftatbestandes zur Kriminalisierung des Betreibens von Darknet-Handelsplattformen ankündigt. Gleichzeitig sehen sich die Strafverfolgungsbehörden durch die Anonymisierungstechnologie des Tor-Netzwerks und der Hidden Services mit neuen Herausforderungen konfrontiert. In Zeiten fortschreitender staatlicher Überwachung der digitalen Sphäre sind diese Anonymisierungstechniken wiederum für die tägliche Arbeit von Journalistinnen und Journalisten weltweit von entscheidender Bedeutung. Diesen Spannungsfeldern widmete sich der Erlanger Cybercrime Tag 2018.

Bereits in den Begrüßungsworten des Dekans der rechts- und wirtschaftswissenschaftlichen Fakultät, *Prof. Hans Kudlich*, und des Veranstalters, *Prof. Christoph Safferling*, wurden viele der genannten Aspekte angesprochen und weitere Fragen aufgeworfen: Wie weit darf eine Vorfeldkriminalisierung im Bereich des Betreibens von Internetplattformen gehen? Welche Ermittlungsmethoden sind im Kampf gegen den Handel mit illegalen Gütern im Darknet erfolgversprechend? Welche neuen Eingriffsbefugnisse benötigen Ermittler? Und wie können wir den Spagat zwischen effektiver Strafverfolgung und Wahrung der Freiheitsrechte im Zeitalter der Digitalisierung schaffen? Mit *Prof. Felix Freiling* (Lehrstuhl für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg), *Jürgen Gause* (Bundeskriminalamt), *Cai Rüffer* (Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität des Bundeslandes Hessen) und *Daniel Moßbrucker* (Reporter ohne Grenzen e.V.) waren herausragende Experten geladen, um diese und weitere Fragen aus technischer, behördlicher, juristischer und menschenrechtlicher Sicht zu beleuchten.

I. Das Tor-Netzwerk: Technische Grundlagen und aktuelle Entwicklungen (*Prof. Dr. Felix Freiling*)

Nach den einleitenden Worten von *Prof. Kudlich* und *Prof. Safferling* übernahm *Prof. Felix Freiling*, Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg, das Rednerpult. Der Vortrag von *Prof. Freiling* führte die Zuhörer in die technischen Grundlagen des sog. Darknets und insbesondere des Tor-Browsers ein:

1. Suchmaschinen als „Gatekeeper" der Informationen im Internet

Der Zugang zum Internet erfolgt für viele Nutzer über die großen Suchmaschinenanbieter. Die meisten Anbieter wie Google und Bing bieten ihren Nutzern durch die Verarbeitung der Nutzerdaten ein personalisiertes, d.h. auf die (vermeintlichen) Interessen des Suchenden abgestimmtes Suchergebnis. Wer „anonymeres" Suchen bevorzugt und dafür auf personalisierte Ergebnisse verzichten will, kann auf Anbieter wie DuckDuckGo zurückgreifen. Angesichts der vielen Millionen Treffer, die bei einigen Suchbegriffen angezeigt werden, ist es überraschend, dass selbst die „großen" Anbieter nur den Zugang zu einem – an der Datenmenge gemessen – relativ kleinen Teil des Internets ermöglichen.

2. Surface Web, Deep Web, Darknet

Der Teil des Internets, den Nutzer über Suchmaschinen erreichen können, ist das sog. Surface Web oder Oberflächennetz. Dieser Begriff ist angesichts der Technik der Suchmaschinenbetreiber treffend: Deren Crawler, die sich durch das Netz bewegen und die Indizes der Anbieter mit Informationen füllen, können tatsächlich mit einem Fischerboot verglichen werden, das mit einem Netz durch das Internet segelt und alle verfügbaren Informationen „abfischt".

„Unter" dem Oberflächennetz findet man das sog. Deep Web. Dieses kann man sich metaphorisch wie die Tiefsee vorstellen: Im Deep Web befinden sich Informationen, die im Internet existieren und über den Browser zugänglich

sind, aber nicht durch Suchmaschinen indexiert oder gefunden werden können. Hierzu gehören vor allem – aber nicht nur – kostenpflichtige Inhalte wie z.B. Datenbanken. Der vom Schöpfer der Begriffe „Surface Web" und „Deep Web" (*Bergmann*) geschätzte Umfang des Deep Web war bereits im Jahr 2001 500 Mal größer als der Umfang des Surface Web. Zudem steigt der Informationsgehalt des Deep Web schneller an als derjenige des Surface Web.

Das Darknet – der Begriff stammt von einem Buch von *Jamie Bartlett* aus dem Jahr 2014 – ist schließlich das „wirklich" versteckte Netz. Grundsätzlich kann man sich das Darknet als Internet-Untergrund vorstellen bzw. in Anlehnung an die bislang verwendeten Metaphern als Meeresboden des Internets. Dort ist es dunkel und es treibt sich allerhand „Getier" herum, das man normalerweise nicht sieht. Auf die Seiten des Darknets kann nur mit spezieller Browser-Software zugegriffen werden. Die Funktionsweise dieser Browser-Software lässt sich gut mit dem Konzept des „Tunnels" erklären: Ein Tunnel ist eine Röhre, in die man hineinlaufen kann. Dann verschwindet die Röhre und kommt irgendwo wieder heraus. Wenn der Tunnel keine Abzweigung hat, kann man einfach hineingehen und auf der anderen Seite wieder heraus kommen. Ein Beobachter kann am Eingang stehen und sehen, wer oder was hineingeht und herauskommt. Falls der Tunnel nah an der Oberfläche ist, wenn es sich zum Beispiel um einen Verkehrstunnel oder dergleichen handelt, dann kann man vielleicht Autos, oder früher die Dampfmaschinen von einem Zug, durchdonnern hören, aber man kann nicht direkt hineinsehen. „Tunnel" ist daher auch der Begriff, den Informatiker für eine verschlüsselte Verbindung benutzen. Dabei kann der Datenverkehr nicht einfach durch Programme wie Wire Shark mitgelesen werden. Ein solcher Tunnel kann zwischen zwei beliebigen Rechnern, unabhängig von deren physischem Standort, aufgebaut werden. Das heißt, Ein- und Ausgang eines solchen Tunnels können an beliebigen Orten auf der Welt sein. Die meisten Webseiten-Betreiber bieten mittlerweile verschlüsselte Verbindungen über „https" an. Bei einer solchen Verbindung kann ein potentieller Angreifer nur sehen, dass zwei Endpunkte miteinander kommunizieren (also den Ein- und Ausgang des Tunnels beobachten und miteinander in Verbindung bringen), jedoch nicht, was kommuniziert wird (also nicht in den Tunnel hineinsehen).

3. Das Tor-Netzwerk

Das Tor-Netzwerk möchte das Problem lösen, dass der Angreifer immer noch sehen kann, wer mit wem kommuniziert. Wie das funktioniert, lässt sich ebenfalls anhand des Tunnelkonzepts erklären: Die grundlegende Idee ist, mehrere Tunnel hintereinander zu bauen und zusätzlich Zwischenstationen einzufügen. Das Tor-Netzwerk besteht aus weltweit ca. 6.000 solcher Zwischenstationen, an denen die Tunnel zusammentreffen und an denen der Datenverkehr seine Richtung ändern kann. Der Tor-Browser wählt für den Datenverkehr zur aufgerufenen Webseite automatisch einen Weg über drei verschiedene Zwischenstationen aus und baut zu diesen bzw. zwischen diesen jeweils verschlüsselte Verbindungen (Tunnel) auf. Gäbe es nun nur eine einzige solche Verbindung, durch die nur der losgeschickte Zug (=Datenverkehr) fährt, dann könnte ein Angreifer durch das Lauschen an den Verbindungen hören, wohin der Zug fährt. Dadurch, dass sehr viele Nutzer sehr viele Züge durch sehr viele Tunnel schicken, entsteht jedoch eine Art „Rauschen". Hierdurch kann der Angreifer die Geräusche eines einzelnen Zuges nicht mehr eindeutig identifizieren. Sie verstecken den konkreten Datenverkehr also im gesamten Datenverkehr, deshalb nennt man das auch „Cover Traffic". Und schließlich können auch die Zwischenstationen (die durch einen Angreifer kontrolliert werden könnten) nicht sehen, wer mit wem kommuniziert. Dies wird dadurch sichergestellt, dass der Datenverkehr durch den Tor-Browser dreifach verschlüsselt wird und jede Zwischenstation nur eine Schicht entschlüsseln kann und nur die Information erhält, wohin sie das Datenpaket weiterschicken soll, nicht jedoch, wo der finale Bestimmungsort ist. Dieses System ist vergleichbar mit der Kommunikation über mehrere Boten, wie man sie zum Beispiel vom Terror-Netzwerk von *Osama Bin Laden* kannte: Dort wurden Nachrichten an einen Boten übergeben, der sich mit einem zweiten Boten an einer verabredeten Stelle traf. Erst der zweite Bote brachte die Nachricht an *Bin Laden*. Der erste Bote wusste nicht, wohin die Nachricht letztendlich gebracht wurde, und der zweite Bote wusste nicht, woher die Nachricht kam. Keiner der Boten kannte den vollständigen Weg des Datenträgers, sodass Quelle und Ziel geheim blieben.

4. Hidden Services im Tor-Netzwerk

Über den Tor-Browser erreicht man auch die sog. Hidden Services. Diese bilden den eigentlichen „Kern" des Darknets oder das Darknet im engeren Sinne. Die Adressen dieser Webseiten enden auf „.onion" und werden nicht von Suchmaschinen gefunden. Bei diesen Hidden Services bleibt – genau wie bei Tor-Nutzern – die IP-Adresse geheim. Dies wird – grob vereinfacht – dadurch erreicht, dass der Tor-Browser nicht „direkt" (also über die drei Zwischenstationen des Tor-Netzwerks) mit den Seiten der Hidden Services kommuniziert, sondern dass Tor-Browser und Hidden Service über Tor-Netzwerkverbindungen einen geheimen Treffpunkt vereinbaren, über den die Kommunikation vermittelt wird. Dieser Treffpunkt ist ein Knotenpunkt im Tor-Netzwerk und heißt „Rendezvous-Point". Die Verbindung zum Rendezvous-Point wird sowohl vom Tor-Browser des Nutzers als auch vom Hidden Service über eine Tor-Netzwerk-Verbindung aufgebaut (also über jeweils drei Zwischenstationen). Das ist der eigentliche Kern des Darknets: Die Kommunikation ist auf beiden Seiten anonym. Diese Anonymisierungstechnologie ist für verschiedene Interessensgruppen attraktiv. Beispielsweise betreiben in manchen Ländern staatskritische Gruppen Server im Darknet, auf denen politische Meinungen ausgetauscht werden. Die Anonymisierung des Servers schützt das Diskussionsforum vor dem Zugriff durch Strafverfolgungsbehörden, falls kritische Bemerkungen über den jeweiligen Staat dort strafbar sind. Mittlerweile betreiben aber auch viele Unternehmen wie z.B. Facebook und verschiedene Suchmaschinen einen Hidden Service. Daneben machen sich aber natürlich auch viele kriminelle Akteure das Tor-Netzwerk zu Nutze. Im sog. Hidden Wiki finden sich die „.onion"-Adressen vieler Hidden Services.

Dort findet man z.B. Marktplätze, auf denen mit allerlei illegalen Gütern wie z.B. gefälschten Kreditkarten, gefälschten Banknoten, gestohlenen Waren, Waffen, falschen Pässen oder Drogen gehandelt wird. Auch illegale Dienstleistungen werden angeboten, man findet beispielsweise Angebote für Auftragsmorde oder manipulierte Bundesligaspiele, auf die man wetten kann.

5. Aktuelle Entwicklungen

Vollständige Anonymität ist jedoch auch im Darknet nicht gewährleistet. Zum einen lassen sich Tor-Nutzer über andere Kommunikationswege verfolgen, wenn diese nicht sehr diszipliniert vorgehen und sich z.B. während der Tor-Nutzung gleichzeitig in ihren Google-Account einloggen. Weiterhin lassen sich Tor-Nutzer mittels des sog. Browser-Fingerprintings de-anonymisieren. Dabei wird versucht, die technischen Charakteristika des verwendeten Browsers (z.B. Bildschirmgröße, Spracheinstellungen, installierte Plug-Ins usw.) zu speichern und später zu einer Wiedererkennung zu verwenden. Nach einiger Forschung in diesem Bereich funktioniert diese Methode mittlerweile recht gut. Weitere Informationen sind auf der Homepage von *Prof. Freiling* zu finden: https://browser-fingerprint.cs.fau.de/?lang=de. Und schließlich gibt es Forschung zu sog. Zeitangriffen, bei denen Netzwerkverkehr korreliert wird. Um bei der Zugmetapher zu bleiben: Wenn der Angreifer den Verdacht hat, dass zwei Personen über Tor kommunizieren, horcht der Angreifer bei der einen Person, ob und wann ein Zug in den Tunnel einfährt und bei der anderen Person, ob und wann ein Zug den Tunnel dort verlässt. Passen die Zeitpunkte unter Berücksichtigung der durchschnittlichen Zuggeschwindigkeit zusammen, gibt es eine gewisse Wahrscheinlichkeit, dass es derselbe Zug ist. Bei häufiger Wiederholung dieses Vorgangs erhöht sich die Wahrscheinlichkeit dafür, dass die beiden tatsächlich miteinander kommunizieren.

6. Diskussion

In der Diskussion wurde – neben einigen Verständnisfragen zum Vortrag – vor allem die Nutzung des Darknets zu legitimen Zwecken thematisiert. *Prof. Freiling* nannte hier die Umgehung der Internetzensur in autokratischen Systemen und anderen nicht-freiheitlichen Staatssystemen (z.B. China) sowie den Schutz der Privatsphäre (z.B. das Verbergen einer Krankheit oder die Kommunikation in einem privaten Forum mit Gleichgesinnten). Auch Browser-Fingerprinting kann gezielt im Rahmen der Strafverfolgung eingesetzt werden. Wenn beispielsweise der eindeutige Browser-Fingerprint eines Straftäters im Rahmen einer Internetermittlung erhoben wurde, weil er etwa gezielt auf eine Webseite gelockt wurde, die durch die Strafverfolgungsbehörden betrieben wird, so kann bei einer Durchsuchung der „Fingerabdruck" des Browsers auf dem Rechner des Beschuldigten genommen werden. Die Übereinstimmung des Fingerabdrucks mit dem Browser-Fingerprint, der vorher im Netz erhoben wurde, ist ein starkes Indiz dafür, dass der seinerzeit aufgezeichnete Zugriff vom beschlagnahmten Rechner aus erfolgte.

II. Darknet und Strafverfolgung – Heute – Erfolge – Herausforderungen (*Jürgen Gause*)

Der technischen Einführung von *Prof. Freiling* folgte ein Bericht von *Jürgen Gause* – Erster Kriminalhauptkommissar im Bundeskriminalamt und Leiter der Internetermittlungen mit den Schwerpunkten Darknet, Kryptowährungen und Social Media – über verschiedene Arten von Darknet-Plattformen sowie Ziele, Möglichkeiten und Herausforderungen der Strafverfolgung im Darknet.

1. Darknet-Plattformen

Das BKA differenziert innerhalb der zu kriminellen Zwecken genutzten Darknet-Plattformen zwischen Foren und Marktplätzen. Ein Forum bietet die Möglichkeit zur Kontaktaufnahme und Vertragsanbahnung. Die Vertragsabwicklung findet jedoch in der Regel außerhalb des Forums über verschlüsselte Messagingdienste statt. Ein Beispiel für ein solches Forum ist „Deutschland im Deep Web" (DiDW), welches der Öffentlichkeit spätestens seit der Meldung, dass der Münchener Amokläufer den Kauf seiner Waffe über dieses Forum initiiert hatte, bekannt ist. Die Betreiber solcher Foren profitieren in der Regel nicht von Verkäufen auf der Plattform. So hat der Administrator von DiDW z.B. um Spenden für den Serverbetrieb, Strom und den Internetanschluss gebeten. Im Gegensatz zu Foren sind Marktplätze rein auf den Kauf und Verkauf von Produkten ausgelegt. Sie funktionieren wie jede andere E-Commerce Plattform wie eBay oder Amazon. Der Plattformbetreiber fungiert in diesem Falle als Mittler und stellt die Infrastruktur für die Geschäfte bereit. In der Regel verdienen die Marktplatzbetreiber durch Provisionssysteme an jedem über die Plattform abgewickelten Geschäft. Gut funktionierende Rating-Systeme sorgen für eine Transparenz der Vertrauenswürdigkeit einzelner Verkäufer sowie der Qualität des Produkts. Hierdurch wird eine gewisse Hygiene auf den Plattformen gewährleistet und das Risiko von Betrügern reduziert. Eine weitere Sicherheit bieten die sog. Treuhandsysteme, die es dem Käufer – ähnlich wie PayPal – ermöglichen, sein Geld bei Bezahlung des Produkts an einen Dritten (den sog. Treuhänder) zu übermitteln, welcher dieses erst bei Erhalt der Ware an den Verkäufer weiterleitet. Hierdurch werden Betrugshandlungen – mit Ausnahme eines sog. Exit-Scams durch den Treuhänder – weitgehend ausgeschlossen.

2. Delikte im Darknet

Insbesondere auf den Darknet-Marktplätzen findet sich eine Vielzahl krimineller Delikte. Das mit Abstand meist verbreitete Produkt sind Betäubungsmittel. *Jürgen Gause* prognostiziert eine Verlagerung des klassischen Straßenhandels auf solche Plattformen in naher Zukunft zu mindestens 70 %. Ausschlaggebend ist die einfache Nutzung solcher Marktplätze sowie die durch den Tor-Browser gewährleistete relative Anonymität, welche das Entdeckungsrisiko reduziert. Aufgrund der von ihnen ausgehenden großen Gefährlichkeit sind zudem Waffen für die Strafermittler sehr wichtig. Eine Renaissance erlebt im Darknet das Falschgeld. Nachdem sich die Fallzahlen

lange Zeit auf einem absteigenden Ast befanden, steigen diese nun aufgrund der simplen Kaufmöglichkeit auf Darknet-Marktplätzen wieder. Andere Plattformen erleichtern wiederum die Arbeit des Falschgeldproduzenten, indem sie beispielsweise Hologramme in perfekter Qualität anbieten. Als Delikt der ersten Stunde kann man den Handel mit Pässen und Ausweisen bezeichnen. Diese Urkundenkriminalität erklärt sich aus der Erforderlichkeit von Pass oder Ausweis zur Anlegung eines Accounts – sei es, um Kontoverbindungen zu ermöglichen oder Zugang zu Packstationen zu erlangen. Absolutes Massendelikt sowohl im Clearnet als auch im Darknet, ist der Handel mit Kreditkartendaten. Ferner ist auf Darknet-Plattformen Cybercrime im engeren Sinne, also Hacking-Angebote, Botnetze etc., zu finden. Auch die Geldwäsche floriert. Kryptowährungen bieten eine sehr gute Möglichkeit, den über das Geschäft erlangten Gewinn in eine Legalwährung umtauschen und nutzen zu können. Ein Delikt der ersten Stunde – nicht nur des Darknets, sondern allgemein des Internets – bildet der Handel mit Kinderpornografie. Dies liegt an der einfachen Austauschmöglichkeit von Fotos und Videos über das Internet. Ferner findet das BKA immer wieder Webseiten im Darknet, die Auftragsmorde offerieren. Die Echtheit dieser Seiten konnte jedoch bislang nicht bewiesen werden. Zusammenfassend lässt sich eine Vielfalt an Delikten im Darknet feststellen, die polizeiliche Ermittlungen erfordern.

3. Ermittlungsmöglichkeiten im Darknet

Die Darknet-Ermittlungen des BKA lassen sich in zwei Zielrichtungen unterteilen. Primär richten sich die Ermittlungen gegen die Administratoren und Betreiber, welche die Plattformen zur Verfügung stellen, weiterentwickeln und perfektionieren. In der Regel werden die Betreiber nicht selbst deliktisch durch den Handel mit illegalen Gütern tätig, sondern stellen nur die Plattform zur Verfügung und profitieren von den einzelnen Verkäufen. Sekundäres Ziel der Ermittlungen sind die sog. User. Diese Ermittlungen erweisen sich als einfacher, weil die User aktiv Handel mit illegalen Gütern betreiben und die Ware irgendwann physisch von A nach B gelangen muss, was einen guten Ermittlungsansatz bietet.

a) Beispiel Hansa Market

Zur Demonstration der Möglichkeiten bei Ermittlungen gegen Administratoren soll der Fall Hansa Market dienen. Der Marktplatz Hansa Market wurde im Sommer letzten Jahres vom BKA in einer international angelegten Operation stillgelegt. Zuletzt war die Plattform unter den Top 3 der Darknet-Marktplätze im Hinblick auf Userzahl, Anzahl der Angebote sowie der inkriminierten Waren. Im Juli 2017 waren ca. 420.000 User, 1.600 Vendoren sowie 30.000 Käufer, die mehr als einen Kauf getätigt haben, registriert und es existierten über 40.000 aktive Angebote verschiedener inkriminierter Waren. Gehandelt wurde insbesondere mit Betäubungsmitteln, aber auch mit digitalen Gütern, Kreditkartendaten, Ausweisen, Falschgeld etc. Waffen und Kinderpornografie waren auf dieser Plattform verboten. Die Ermittlungen des BKA gegen die Administratoren von Hansa Market begannen effektiv im Januar 2017. Zu diesem Zeitpunkt war es der niederländischen Polizei durch Vorermittlungen gelungen, den Zielserver des Hidden Services zu identifizieren. Dies eröffnete der deutschen Polizei neue strafprozessuale Möglichkeiten. Ziel der internationalen Ermittlungen war die Identifizierung der Administratoren und im Idealfall ein administrativer Vollzugriff auf die Plattform. Dieser gelang und ermöglichte einen temporären polizeilichen Weiterbetrieb der Plattform, wodurch weitere User identifiziert werden konnten, bevor die Plattform final abgeschaltet wurde. Im Gegensatz zum niederländischen Recht ist dieses Vorgehen nach der deutschen Rechtsordnung nicht zulässig. Aus diesem Grund war die internationale Zusammenarbeit im Fall Hansa Market für die deutschen Strafverfolgungsbehörden besonders wichtig. Einen Umweg mussten die Ermittler nicht nur bei den strafprozessualen Maßnahmen wählen, sondern auch bei der Begründung des Tatverdachts. Da das Betreiben einer Darknet-Plattform in Deutschland nicht eigenständig mit Strafe bedroht ist, mussten sich die Ermittler mit einem Verstoß gegen das BtMG behelfen. Die Ermittlungen waren letztendlich erfolgreich und es konnten zwei Administratoren auf der Führungsebene identifiziert werden, die von bis zu drei Moderatoren gegen monatliche Bezahlung unterstützt wurden. Bei den zwei Administratoren handelte es sich um deutsche Staatsangehörige mit guten IT-Kenntnissen. Parallele Ermittlungen der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) haben ergeben, dass die zwei Administratoren auch die Internetplattform „Lesen und Lauschen“ (Lul.to) betrieben. Auf dieser Plattform wurden E-Books und Hörbücher in illegaler Weise hochgeladen und zum Download bereitgestellt. Der Tatverdacht lautete hier: Bildung einer kriminellen Vereinigung, Computerbetrug und Urheberrechtsverletzung.

b) Problemstellungen

Bei solchen Ermittlungen im Darknet ergeben sich verschiedene Problemstellungen für die Strafverfolgungsbehörden. Bis zur Identifizierung der Administratoren sind zunächst technische Ermittlungen, die Informatiker erfordern, notwendig. Neben den technischen Ermittlungen spielt bei der Identifizierung der Administratoren der Faktor Mensch eine Rolle. So kamen die Ermittler im Fall von Hansa Market den Administratoren auf die Spur, weil sie auf dem Server, auf dem sie ihren Hidden Service betrieben, einen unverschlüsselten Privatchat mit reichlich persönlichen Informationen abgelegt hatten. Ist der Zielserver identifiziert, so stehen den Ermittlern in der Regel alle verdeckten strafprozessualen Maßnahmen zur Verfügung, über die sie auch in der analogen Welt verfügen. Ziel der sich anschließenden Ermittlungen ist die Erhärtung des Tatverdachts sowie eine entsprechende Vorbereitung offener strafprozessualer Maßnahmen zur Erreichung der administrativen Übernahme der Plattform. Der administrative Vollzugriff ist eine kriminaltaktische Maßnahme, bei der die Ermittler versuchen, auf den Rechner zuzugreifen und im besten Fall die Plattform zu übernehmen. Ein solcher temporärer polizeilicher Weiterbetrieb ist in Deutschland rechtlich nicht zulässig, weshalb die Ermitt-

ler hier auf eine Zusammenarbeit z.B. mit den niederländischen Behörden angewiesen sind. Den Abschluss der Ermittlungen bildet die finale Abschaltung der Darknet-Plattform. Daneben bereiten Kryptowährungen im Rahmen von digitalen Finanzermittlungen Schwierigkeiten. Zunächst muss das inkriminierte Vermögen festgestellt werden, um dieses anschließend zu sichern und abzuschöpfen. Im Fall der Administratoren von Hansa Market und Lul.to konnten die Ermittler einen Gewinn aus dem Betrieb beider Plattformen von über 1.400 Bitcoins sicherstellen. Dies entspricht einem momentanen Wert von ca. 10 Millionen Euro. Der Staat steht nun vor dem Problem, wie er diese Bitcoins wieder veräußern kann. So stellt sich die Frage, was mit dem Kurs passieren würde, wenn der deutsche Staat nun 1.400 Bitcoins zum Verkauf einstellt und ob er sich dann gegebenenfalls wegen Kursmanipulation strafbar machen könnte. Mit all diesen Problemen sehen sich die Strafverfolgungsbehörden bei Ermittlungen im Darknet konfrontiert.

4. Herausforderungen und Ausblick

Die sich bei Darknet-Ermittlungen stellenden Herausforderungen begründen in mehrerlei Hinsicht einen Handlungsbedarf. Zum einen sind Aus- und Fortbildungen der Polizei zur Gewährleistung einer grundlegenden Kompetenz jedes Kriminalbeamten erforderlich. Darüber hinaus erfordert die polizeiliche Arbeit die Mitwirkung von Informatikern (sog. Cyberanalysten). Weitere Schwierigkeiten bereitet das Recht, insbesondere das Straf- und Strafprozessrecht. Als besonders wichtig erachtet *Jürgen Gause* eine Strafbarkeit von Administratoren und Betreibern. Derzeit behelfen sich die Strafverfolgungsbehörden mit Spezialgesetzen wie dem BtMG. Auf Initiative des BKA wurde im Koalitionsvertrag die Prüfung der Erforderlichkeit eines eigenen Straftatbestandes aufgenommen. Angestrebt wird ein Straftatbestand, der das Zurverfügungstellen und administrative Tätigwerden bezüglich einer Seite wie Hansa Market unter Strafe stellt und die Nutzung strafprozessualer Mittel durch eine Aufnahme in den Katalog des § 100a StPO ermöglicht. Ferner fordert die hohe Dynamik der Technik die Entwicklung und den Einsatz innovativer Tools durch die Strafverfolgungsbehörden, um die Anonymität von Kriminellen aufzuheben und Serverstrukturen von Hidden Services offenzulegen. Eine Herausforderung und eine Chance zugleich bieten außerdem Kooperationsformen verschiedener Strafverfolgungsbehörden. So sind flexible Zusammenarbeitsmodelle sowohl auf nationaler als auch auf internationaler Ebene für erfolgreiche Ermittlungen im Darknet sehr wichtig.

5. Diskussion

Zentrales Thema der Diskussion war der – für deutsche Behörden unzulässige – Weiterbetrieb von Hansa Market durch niederländische Behörden und die Nutzung der hierdurch erlangten Daten durch deutsche Strafverfolgungsbehörden. Es wurde die Frage aufgeworfen, ob ein solches Vorgehen nicht den deutschen Rechtsstaat unterlaufe. Aus polizeilicher Sicht ist wiederum die Erforderlichkeit solch „innovativer" Maßnahmen zu berücksichtigen, die sich aus der rasanten technischen Entwicklung, mit welcher der deutsche Gesetzgeber nicht Schritt halten kann, begründet. Ferner wurde debattiert, ob bzw. wie sich die Abschaltung eines gesamten Forums rechtfertigen lässt, das neben inkriminierten Inhalten auch (größtenteils) der freien Meinungsäußerung dient. Bezogen auf DiDW wies *Jürgen Gause* u.a. auf den politischen Druck hin, sowie dass sich eine Differenzierung zwischen legalen und illegalen Inhalten allein aus technischen Gesichtspunkten schwierig gestalte.

III. Rechtliche Herausforderungen bei Ermittlungen im Darknet (*Cai Rüffer*)

Aufbauend auf dem Vortrag von *Jürgen Gause* über tatsächliche Schwierigkeiten bei Ermittlungen gegen die Underground Economy im Darknet ging Staatsanwalt *Cai Rüffer* von der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) des Bundeslandes Hessen auf einige rechtliche Herausforderungen ein.

1. Verschiedene Täter: Käufer, Verkäufer, Betreiber

Die Täter der Underground Economy des Darknets lassen sich in drei Kategorien einteilen, bei denen sich unterschiedliche juristische Fragen stellen. „Ganz unten" in der Hierarchie stehen die Käufer, die Betäubungsmittel, Waffen, Falschgeld und sonstige Güter auf den Darknet Marktplätzen erwerben. Den ökonomischen Gegenpart stellen die sog. Vendoren und Powerseller dar. Diese verkaufen unter Nutzung von Händleraccounts auf den Marktplätzen die o.g. Waren. An der Spitze finden sich die Administratoren und Moderatoren der Darknet-Marktplätze, die sog. Betreiberebene. Die Ermittlungen gegen die verschiedenen Tätergruppen lassen sich am besten am Beispiel des – auch sehr praxisrelevanten – Betäubungsmittelhandels darstellen:

a) Ermittlungen gegen Käufer

Bei Ermittlungen gegen „einfache" Käufer stellt sich bereits zu Beginn die Frage, ab wann eigentlich ein Versuch des Erwerbs von Betäubungsmitteln nach § 29 Abs. 1 Nr. 1 BtMG vorliegt und somit strafrechtliche Ermittlungen aufgenommen werden können. Auf großen Plattformen wie Hansa Market gibt es zwischen 30.000 und 50.000 Käuferaccounts. Die bloße Anmeldung genügt jedoch sicherlich noch nicht, um von einem Versuchsbeginn des Erwerbs auszugehen. Ein Versuchsbeginn liegt strafrechtlich erst vor, wenn zwischen der vorgenommenen Handlung des Täters und der von ihm angestrebten Deliktsvollendung keine weiteren wesentlichen Zwischenschritte mehr liegen und subjektiv die Schwelle zum „Jetzt-geht's-los" überschritten ist. Problematisch ist im Kontext der Underground Economy, dass die meisten der großen Handelsplattformen ein sog. Escrow- oder Multisig-Verfahren verwenden. Darunter versteht man einen Treuhandservice, bei dem der Betreiber ein Treuhandkonto für Bitcointransaktionen zur Verfügung stellt. Die Ware wird erst ausgeliefert, wenn dort ein Zahlungsein-

gang des Käufers verzeichnet wird und die Bitcoins werden erst an den Verkäufer weitergeleitet, wenn die Ware beim Käufer ankommt. Das bedeutet, dass der Käufer nicht bereits beim Einlegen der Ware in den Warenkorb und dem Anklicken des „Bestell-Buttons" davon ausgehen kann, dass er die Ware tatsächlich erhält. Als wesentlicher Zwischenschritt ist noch die Überweisung der Bitcoins auf das Treuhandkonto notwendig. Erst dann ist aus Sicht des Käufers die Schwelle zum „Jetzt-geht's-los" überschritten und es liegt ein Versuchsbeginn vor. Aus Perspektive der Ermittler ist dies natürlich misslich: Bei einer reinen Darknet-Streife durch die Marktplätze können diese nicht erkennen, welcher Käufer für einen solchen Kauf bereits Bitcoins überwiesen hat. Einen Ansatzpunkt für Ermittlungen können jedoch die hochprofessionell betriebenen Bewertungssysteme der Marktplätze bieten: Dort kann eingesehen werden, wer bei wem was gekauft hat. Dies kann einen Anfangsverdacht für einen bereits abgewickelten Erwerb nach § 29 Abs. 1 Nr. 1 BtMG begründen.

Manchmal haben die Ermittler auch „Glück" und der Käufer versucht, Waren bei einem Scheinverkäufer der Polizei (Verdeckter Ermittler oder noeP) zu kaufen. Allerdings stellt sich das Problem des Versuchsbeginns und damit des Anfangsverdachts auch hier: Im reinen Anklicken der Ware oder Legen in den Warenkorb kann noch kein Versuchsbeginn gesehen werden. Anders ist dies nur, wenn ein Verbrechenstatbestand, z.B. das Handeltreiben mit einer nicht geringen Menge nach § 29a Abs. 1 Nr. 2 BtMG im Raum steht (bei Absicht der Weiterveräußerung genügt auch bereits der Erwerb als Tathandlung für das Handeltreiben,[1] Anmerkung der Autoren). Dann kann über den Tatbestand des Versuchs der Beteiligung nach § 30 StGB ein Anfangsverdacht nach § 152 Abs. 2 StPO begründet werden.

b) Ermittlungen gegen Verkäufer

Bei Vendoren und Powersellern ist die Begründung eines Anfangsverdachts einfacher. Neben den Ratings, aus denen auf vergangene Straftaten geschlossen werden kann, können auch die von den Verkäufern online verfügbar gemachten Warenangebote zur Begründung herangezogen werden. Die meisten Plattformen haben AGBs, in denen der Versand der gekauften Ware innerhalb einer kurzen Zeit – zumeist innerhalb von 24 – 48 Stunden nach der Bestellung – verlangt wird. Wenn der Verkäufer überwiegend positive Ratings hat, kann davon ausgegangen werden, dass er die angebotene Ware bereits besitzt. Andernfalls könnte er die Lieferzeiten wohl nicht einhalten. Da bereits der Besitz der Ware zur Weiterveräußerung den Tatbestand des Handeltreibens erfüllt, kann ein Anfangsverdacht nach § 29 Abs. 1 Nr. 1 BtMG bejaht werden. Zur weiteren Ermittlung wird oftmals zunächst ein Scheinkauf beim entsprechenden Händler durchgeführt – genau wie bei entsprechenden Ermittlungen in der Realwelt. Dabei liegt auch keine „agent provocateur"-Problematik vor, da der Händler durch sein Angebot seine Bereitschaft zum Verkauf bereits deutlich gemacht hat. Wird eine nicht geringe Menge scheingekauft, erlangt der Tatverdacht sogar Verbrechensqualität nach § 29a Abs. 1 Nr. 2 BtMG. Gelingt eine Identifikation des Händlers, erfolgt im Regelfall anschließend eine Durchsuchung bei ihm. Können dabei keine Betäubungsmittel aufgefunden werden und können – z.B. weil ein Zugriff auf den Rechner des Beschuldigten misslingt – auch auf andere Weise keine konkreten Verkäufe nachgewiesen werden, besteht immer noch die Möglichkeit einer Anklage nach § 30 Abs. 2 StGB (Bereiterklären zur Verbrechensbegehung) oder § 29 Abs. 1 Nr. 8 BtMG (Werbung für Betäubungsmittel) allein durch das Verkaufsangebot.

c) Ermittlungen gegen Betreiber der Darknet-Handelsplattformen

In Bezug auf die Administratoren und Moderatoren der großen Handelsplätze stellt sich das zentrale Problem, dass es bislang keinen eigenständigen Straftatbestand gibt, der das Betreiben krimineller Infrastrukturen unter Strafe stellt. Auch die Begründung einer Beihilfestrafbarkeit ist in der Praxis nicht immer einfach. Zunächst sind die modernen Handelsplattformen in hohem Maße automatisiert, d.h. nach der Programmierung und Inbetriebnahme sind kaum noch Handlungen der Betreiber vonnöten. Dies führt dazu, dass die Betreiber oftmals – trotz zehntausender über die Plattform abgewickelter Verkäufe – nur wegen einer einzigen Beihilfetat verfolgt werden können. Außerdem gibt es häufig ein Nachweisproblem: Wenn man nicht digitalforensisch exakt nachweisen kann, welcher Administrator/Moderator welchen Teil der Plattform programmiert/gepflegt hat, müsste man bei jedem Beteiligten wegen des „in dubio pro reo"-Prinzips davon ausgehen, dass er/sie die jeweilige Handlung gerade nicht vorgenommen hat. Anders als bei der Mittäterschaft können im Rahmen einer Beihilfestrafbarkeit auch nicht wechselseitig Tatbeiträge zugerechnet werden, da § 25 Abs. 2 StGB nicht gilt. Speziell beim Handel mit Betäubungsmitteln ist jedoch oft der Gang über eine täterschaftliche Begehungsweise von § 29 Abs. 1 Nr. 10 BtMG (öffentliche Mitteilung einer Gelegenheit zum Erwerb von Betäubungsmitteln) möglich und wird in der Praxis auch angewendet.

2. Strafprozessrechtliche Herausforderungen

Aus strafprozessrechtlicher Sicht stellen sich derzeit vor allem zwei Probleme: Die Herausgabe von retrograden Sendungsdaten durch Post- und Paketdienstleister und die Erlangung von Daten von Dienstleistern, die keinen Sitz in Deutschland haben.

a) Retrograde Herausgabe von Sendungsdaten

Die gekauften Waren, z.B. Drogen und Waffen, werden sehr häufig durch Paket- und Postdienstleister versendet. Daher sind die Sendungsdaten solcher Pakete – Wo kommen diese her und wo gehen diese hin? – von großer ermittlungstechnischer Relevanz. Diese Daten kann man

[1] Vgl. *Patzak,* in: Körner/Patzak/Volkmer, BtMG, 8. Aufl. (2016), § 29, Teil 4, Rn. 46 m.w.N.

von den Dienstleistern auch erlangen. Problematisch ist jedoch, auf welche Rechtsgrundlage dies gestützt werden kann. In einer aktuellen Entscheidung hat der Ermittlungsrichter beim *BGH* entschieden,[2] dass § 95 StPO – auf die in der Praxis bislang solche Anfragen gestützt wurden – keine taugliche Rechtsgrundlage sei. Als Grund wurde angeführt, dass die retrograde Abfrage von Sendungsdaten ein Eingriff in Art. 10 Abs. 1 GG darstelle und deshalb die Eingriffsnorm den Eingriff in das Postgeheimnis bereichsspezifisch und normenklar regeln müsse. Dies sei angesichts der Existenz von § 99 StPO bei § 95 StPO nicht der Fall. Allerdings hat das *BVerfG* bereits 2009 (in der Entscheidung zur E-Mail-Beschlagnahme,[3] Anmerkung der Autoren) entschieden, dass die §§ 94 ff. StPO eine taugliche Rechtsgrundlage für Eingriffe in Art. 10 Abs. 1 GG sein können.

b) Zugriff auf Daten im Ausland

Ermittlungsrelevante Daten – insbesondere von Telemediendiensten wie Google, Amazon & Co – befinden sich häufig im (nicht europäischen) Ausland. Deshalb ist es oftmals schwierig und langwierig, die entsprechenden Daten zu erhalten. In einigen Fällen misslingt dies auch vollständig. Möglich ist bislang vor allem der Weg über Rechtshilfeersuchen, wobei auch diese Verfahren des Öfteren – insbesondere bei dezentraler Speicherung von Daten – an ihre faktischen Grenzen stoßen. Die Strafverfolgungsorgane setzen große Hoffnungen in das Zustandekommen einer europäischen Regelung für einen direkten Zugriff auf Daten, die auf einem Server in einem Mitgliedstaat gespeichert sind, um die Ermittlungsmöglichkeiten zu verbessern.

Wenn Ermittlungen schließlich erfolgreich verlaufen, werden oftmals Bitcoins – die als Hauptzahlungsmittel im Darknet verwendet werden – nach § 111b StPO beschlagnahmt oder es wird ein Arrest nach § 111e StPO verfügt. Die Höhe eines Arrests kann dabei nach § 73d StGB auch geschätzt werden, wobei auch auf Daten der Handelsplattformen wie z.B. das durchschnittliche Transaktionsvolumen der Verkäufe zurückgegriffen werden kann. Schwierigkeiten ergeben sich oft bei der tatsächlichen Sicherstellung der Bitcoins, da die Ermittlungsbehörden hierfür den Zugriff auf die meist passwortgeschützten Wallets der Beschuldigten benötigen. Dies gelingt oft nur, wenn der Beschuldigte kooperiert. Die Veräußerung der Bitcoins ist nunmehr nach § 77a BayStVollstrO Zentralstellenaufgabe, sodass die bisherige Praxis von Notveräußerungen durch die sicherstellenden Behörden zumindest in Bayern wohl der Vergangenheit angehört. Bei der Veräußerung liegen auch für die handelnden Beamten gewisse Haftungsrisiken, weil z.B. bei einem Tippfehler die Bitcoins – wegen der dezentralen Struktur der Blockchain – für immer verloren gehen können.

3. Diskussion

In der Diskussion wurde u.a. über die technischen Herausforderungen im Rahmen der Nachverfolgung von Transaktionen mit virtuellen Währungen wie Bitcoin und Monero gesprochen. Außerdem wurde die Schwierigkeit des Nachweises eines Tatvorsatzes bei einer großen Vielzahl von Einzeltaten diskutiert und die Frage eines Rücktritts des Käufers nach Einzahlung des Kaufpreises auf das Treuhandkonto der Handelsplattform thematisiert.

IV. Das Darknet als Baustein der Demokratie: Bedeutung von Anonymität für die Pressefreiheit (*Daniel Moßbrucker*)

Nach den Vorträgen über die Nutzung des Darknets durch Kriminelle beleuchtete *Daniel Moßbrucker* die „helle Seite" des Darknets im Sinne des Einsatzes dieser und ähnlicher Technologien zugunsten der Meinungs- und Pressefreiheit. *Daniel Moßbrucker* ist freier Journalist und Security-Trainer sowie Referent für Internetfreiheit bei der Menschenrechtsorganisation Reporter ohne Grenzen e.V.

1. Bedrohung der Pressefreiheit im Digitalen

Die zentrale Norm für Journalisten ist § 53 StPO, welche u.a. das Schweigerecht von Journalisten in der analogen Welt vor Gericht regelt. Nur bei wenigen Straftaten herrscht eine Aussagepflicht, die jedoch der Schranke unterliegt, dass die Identität eines Informanten niemals preisgegeben werden muss. Dieser absolute Informantenschutz im offenen Ermittlungsverfahren wird durch das Durchsuchungs- und Beschlagnahmeverbot flankiert. In der analogen Welt ist dieses absolute Zeugnisverweigerungsrecht wertvoll und wichtig. Im Digitalen hat sich die Lage jedoch verändert. Maßgebliche Norm ist dort § 160a StPO, welche die Zulässigkeit einer verdeckten Ermittlung gegen Journalisten als eine Einzelfallentscheidung ausgestaltet. Bei dieser Entscheidung muss der Schutz der Pressefreiheit gegen das Strafverfolgungsinteresse des Staates abgewogen werden. Dies ist mit dem grundsätzlichen Vertrauen in den Quellenschutz von Journalisten, welches das *BVerfG* im Nachgang zur Spiegelaffäre gefordert hatte, schwer vereinbar. Problematisch ist insbesondere die Anwendung des § 160a StPO auf immer mehr Ermittlungsmethoden. So wurden allein in den letzten zwei Jahren der großen Koalition zahlreiche Gesetze erlassen, die entweder bestehende Ermittlungsbefugnisse erweitert oder neue geschaffen haben.

Zunächst wurde im Jahr 2015 die Vorratsdatenspeicherung eingeführt, welche aufgrund der zwangsläufigen Mitspeicherung von Kommunikationsdaten von Journalisten eine der größten Sorgen von Journalistenverbänden darstellt. Gleichzeitig wurde der Straftatbestand der Datenhehlerei geschaffen, der v.a. den Handel mit kriminellen Daten verbieten sollte. Nach Ansicht von Reporter ohne Grenzen wird hiervon jedoch auch das Leaken von Daten an Journalisten erfasst, weshalb die Organisation eine Verfassungsbeschwerde gegen diese Norm eingereicht hat. Zudem wurde der Verfassungsschutz reformiert und hierdurch der Datenaustausch intensiviert. Auf europäischer Ebene geschah das Ganze durch die Euro-

2 *BGH*, NJW 2017, 680.

3 BVerfGE 124, 43.

polreform. Des Weiteren wurde das Anti-Terror-Paket erlassen, welches den anonymen Kauf von SIM-Karten verhindert. Dies bedeutet für Journalisten eine große Einschränkung des Berufsalltags, da sie auf Recherchereisen zur Gewährleistung ihrer Anonymität auf solche SIM-Karten-Handys angewiesen waren. Darüber hinaus wurde das BND-Gesetz reformiert und die anlasslose Überwachung ausländischer Journalisten ermöglicht. Außerdem wurde die Behörde ZITiS geschaffen, um Methoden zum Brechen von Verschlüsselung institutionalisiert zu entwickeln. Dem folgte die EU-Anti-Terrorrichtlinie, welche die Quellen-TKÜ auf EU-Ebene erlaubt. Ferner wurde das Bundesdatenschutzgesetz reformiert und u.a. die unabhängige Kontrolle des Bundesnachrichtendienstes durch die Datenschutzbeauftrage gestrichen. Auf europäischer Ebene wurde die Fluggastdatenspeicherung umgesetzt, die auch Recherchereisen von Journalisten mit dem Flugzeug erfasst. Zudem dürfen die Geheimdienste mittlerweile automatisiert biometrische Passfotos abgleichen. Zuletzt wurde der Staatstrojaner im Strafverfahren eingeführt.

Führt man sich diese Erweiterungen der Eingriffsbefugnisse vor Augen, wird die Problematik des bloß relativen Schutzes durch § 160a StPO deutlich. Im Gegensatz zu dem absoluten Schutzrecht in der analogen Welt wird alles Neue der digitalen Welt – bestenfalls – an das relative Schutzrecht des § 160a StPO gekoppelt. In vielen Fällen, insbesondere bei Datenbanken, wird auf journalistische Schutzrechte komplett verzichtet. So mangelt es in den entsprechenden rechtlichen Bestimmungen an Schutzvorkehrungen für Journalisten, die aufgrund einer regelmäßigen Teilnahme an Demonstrationen naturgemäß potentiell häufiger angezeigt werden. In der Folge kam es zum Akkreditierungs-Skandal beim G20-Gipfel in Hamburg, bei dem zahlreichen Journalisten aufgrund der Erfassung ihrer Person in einer Datenbank der Zutritt verwehrt wurde. Dies bedeutet für die journalistische Arbeit eine sukzessive Schwächung im Digitalen. Selbst wenn sich einzelne Maßnahmen von Überwachung vor dem Hintergrund internationaler Bedrohungen rechtfertigen könnten, bedarf es dann auf der anderen Seite zwingend Kompensationen, die bislang nicht erfolgt sind. So wurden im letzten Koalitionsvertrag Änderungen im Rahmen des sog. Hinweisgeberschutzes angekündigt, aber nicht umgesetzt. Im aktuellen Koalitionsvertrag finden diese schon keine Erwähnung mehr. Deutschland ist damit eines der wenigen europäischen Länder, das Whistleblowern keinen rechtlichen Schutz bietet. Aufgrund dieser mangelnden Schutzrechte ergibt sich für Journalisten eine Notwendigkeit, in ihrem Alltag verstärkt auf Technologie zu setzen.
Zusammenfassend lautet die erste These: *Durch den technologischen Wandel und abgeschwächte Schutzrechte für Journalisten ist es schwieriger geworden, Quellen zu schützen. Digitale Selbstverteidigung – wozu auch die Darknet-Technologie gehört – wird aufgrund von politischen Entwicklungen essenziell.*

2. Darknet-Technologien als Freiheitsräume

Das Darknet bietet nicht nur Kriminellen, sondern auch Freiheitskämpfern verschiedene Nutzungsmöglichkeiten. Zum einen kann das Darknet – als Synonym für alle Formen sicherer und anonymer Kommunikation – als Schutz vor Verfolgung dienen, als sog. High-End Security für Journalisten und Aktivisten, die in extremen Umfeldern erheblicher Bedrohung ausgesetzt sind. Ein Beispiel für solch extreme Umstände bildet der Fall *Hisham Almiraat*, den Reporter ohne Grenzen betreut hat. *Almiraat* hat im arabischen Frühling zu Bloggen begonnen, wurde dann verfolgt, seine Geräte wurden gehackt und letztendlich wurde er aus dem Land vertrieben. Mittlerweile wird er per Haftbefehl wegen Unterstützung von Terroristen gesucht – ein Vorwurf, den *Daniel Moßbrucker* als „völlig absurd" bezeichnet. Zu seinem eigenen Schutz nutzt *Almiraat* die Darknet-Technologie, in dem er einen eigenen Hidden Service betreibt und seine Kommunikation schwerpunktmäßig hierüber laufen lässt. Seine gesamten Daten speichert er auf diesem Server, so dass man im Falle seiner Verhaftung physisch nicht an diese Daten gelangt.

Neben dem Schutz in solchen Extremfällen ist bei der Arbeit in Krisengebieten der Teiltransfer sehr wichtig. Mithilfe von Darknet-Technologien bzw. zensurresistenten Upload-Plattformen im Darknet wird in Risikogebieten Material (meist Fotos oder Videos) hochgeladen und so außer Landes transportiert. Als Beispiel hierfür kann die Gruppe „Raqqa Is Being Slaughtered Silently" angeführt werden. Als der IS Raqqa als „Hauptstadt" des sog. Kalifats ausrief und dort mordete, waren noch zehn bis zwölf Journalisten der Gruppe vor Ort. Diese nutzten eine Hidden Service Technologie, um ihr Videomaterial hochzuladen. Gruppenmitglieder, die sich bereits im Exil befanden, luden dieses Material dann anonym herunter und übermittelten es an westliche Medien. Eine direkte Veröffentlichung der Videos im Darknet wäre aufgrund der geringen Reichweite nicht erfolgversprechend gewesen. Das Darknet dient vielmehr als eine Brücke in die freie Welt. Dieser Anwendungsfall von Hidden Services ist relativ populär und wird mittlerweile beispielsweise auch in der Türkei von vielen Medien genutzt – v.a. im syrisch-türkischen Kriegsgebiet.

Von der Empfängerseite wird die Darknet-Technologie hingegen als anonymer Briefkasten verwendet. Ca. 180 renommierte Medien bedienen sich mittlerweile dieser Möglichkeit, um Whistleblowern eine sichere Übermittlung von Informationen zu gewährleisten. Die Medien bewerben diese anonymen Briefkästen im normalen Netz mit dem Hinweis, dass ein anonymes Hochladen von Daten lediglich die Nutzung des „Tor Browsers" und das Eingeben der genauen URL erfordert. Mittlerweile gebrauchen auch deutsche Medien – namentlich die Süddeutsche, Spiegel Online, Heise – diese Möglichkeit. Allerdings ist das Bedürfnis in Deutschland aufgrund der herrschenden hohen rechtsstaatlichen Standards verhältnismäßig gering.

Eine weitere vielversprechende Nutzungsmöglichkeit der Darknet-Technologie ist der Gebrauch eines Hidden Service als Kommunikationstechnologie. Ein Beispiel hierfür ist die App „Ricochet". Diese ähnelt WhatsApp, aber installiert ohne Zutun des Nutzers einen eigenen „Mini Hidden Service" auf das jeweilige Smartphone. Wenn der

Nutzer chattet, läuft seine Kommunikation automatisch anonym und verschlüsselt über einen Hidden Service.

Diese vier Möglichkeiten einer Nutzung des Darknets für positive Zwecke im Blick haltend, formuliert Daniel Moßbrucker seine zweite These: *Hidden Services verbinden einzelne Aspekte digitaler Sicherheit zu ihrer extremsten Form. Nur weil ihr positiver Nutzen weniger öffentlich ist als der kriminelle Missbrauch der Technologie, darf dieses Freiheitspotenzial nicht negiert werden.*

3. Internationale Implikationen deutscher Sicherheitspolitik

Zuletzt stellt sich die Frage, wie die deutsche Politik diese zahlreichen Sicherheitsgesetze – man kann mittlerweile wohl von einer Art Überwachungslobbyismus sprechen – rechtfertigt. Ein gutes Beispiel deutscher Sicherheitspolitik ist die Vorratsdatenspeicherung. Diese wurde im Oktober 2015 eingeführt und sollte Anfang 2017 in Kraft treten. Im November 2015 ereigneten sich die Terroranschläge in Paris mit über hundert Toten. Noch in der Anschlagsnacht erließ die Gewerkschaft der Polizei folgendes Statement: „Das eng gefasste Gesetz zur Vorratsdatenspeicherung muss überdacht werden. Die Polizei muss Anschläge wie die in Paris unter allen Umständen verhindern." Dieses Statement zeigt, wie öffentliche Angst missbraucht wird, um eigene Interessen hinsichtlich eines Instruments durchzusetzen, über dessen Auswirkungen und Effektivität es aus damaliger Ermittlersicht noch keinen Erfahrungswert gab. Dieses oder ähnliches Vorgehen (wie z.B. die Argumentation mit Kindesmissbrauch) wird oftmals von der Politik gewählt, um Sicherheitspolitik durchzusetzen, was die Arbeit der Vertreter von Freiheitsrechten maßgeblich erschwert. Als weiteres Beispiel solcher Sicherheitspolitik kann der Staatstrojaner angeführt werden. Auch in dieser Debatte wird von Seiten der Strafermittler immer mit internationalem Terrorismus, organisiertem Verbrechen oder Cybercrime argumentiert. Dies wirft die Frage auf, warum der Staatstrojaner im regulären Strafverfahren erforderlich ist, schließlich konnte das BKA die Methode für die genannten Delikte ja längst nutzen. Die Argumentation ist stets die gleiche und es mangelt an einer Analyse des Nutzens der geschaffenen Eingriffsbefugnisse. Der Staatstrojaner erlaubt auch das „Einhacken" in Journalistenhandys. Dem Protest hiergegen wurde damit begegnet, dass der Trojaner nach anfänglichen Schwierigkeiten zur Einhaltung der verfassungsrechtlichen Grenzen künftig in Deutschland programmiert werden soll. Allerdings ist die eigene Entwicklung gescheitert und so wurde doch auf einen Trojaner der Firma „FinFisher" zurückgegriffen. Dieses Gerät wird wiederum von Reporter ohne Grenzen zahlreich auf Handys von Aktivisten im Nahen Osten gefunden. Die deutsche Gesetzgebung finanziert so einen Markt, der Auswirkungen in der ganzen Welt hat. Die Unterstützung des Aufbaus dieser Industrie – der Ausrüstung von Autokratien mit Überwachungsinstrumenten – erhöht gleichzeitig den Druck der Gegenseite und fördert somit die Entwicklung von Tor oder ähnlichen Technologien.

Hieraus ergibt sich die letzte These: *Debatten über die Methoden der digitalen Kriminalitätsbekämpfung können nicht allein national diskutiert werden. Deutschland finanziert mittlerweile eine Überwachungsindustrie, die mit Autokraten Geschäfte macht. Damit befördert es paradoxerweise die Weiterentwicklung des Darknets.*

Daniel Moßbrucker schließt seinen Vortrag mit folgendem Zitat von Benjamin Franklin: „Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren."

4. Diskussion

In der Diskussion wurde insbesondere die Rechtfertigung der angesprochenen Eingriffsbefugnisse thematisiert. Von behördlicher Seite wurde betont, dass die Nutzung von Kryptographie durch Private von staatlicher Seite aus durchaus gewollt sei, aber Maßnahmen die Handlungsfähigkeit des Staates und eine effektive Strafverfolgung sicherstellen müssen. Anwesende Strafermittler wiesen auf die hohen Voraussetzungen der Durchführung grundrechtsrelevanter Maßnahmen im Einzelfall und gute Überprüfungsmechanismen hin. Dem Argument, dass der Zweck dieser Maßnahmen gerade nicht die Behinderung der journalistischen Arbeit sei, begegnete *Daniel Moßbrucker* mit der Gegenfrage, warum nicht stets Schutzrechte für Journalisten aufgenommen werden. Daneben war die Unbestimmtheit des Journalistenbegriffs Gegenstand der Debatte. Diese begründet einerseits eine Missbrauchsgefahr, andererseits ist sie zur Gewährleistung einer umfassenden, von staatlichen Akteuren unabhängigen Pressefreiheit notwendig.

V. Abschlussdiskussion

Die vom Veranstalter, *Prof. Christoph Safferling*, geleitete Abschlussdiskussion drehte sich maßgeblich um die Quellen-TKÜ (sog. Staatstrojaner) und mögliche Alternativen sowie den staatlichen Umgang mit Sicherheitslücken. *Prof. Safferling* griff die vorangegangene Diskussion durch einige Hinweise zur Quellen-TKÜ und zu den widerstreitenden Interessen auf: Die Quellen-TKÜ wurde als Reaktion auf den technischen Wandel und die hierdurch entstandenen Grenzen der regulären TKÜ bei verschlüsselter Kommunikation eingeführt. Kriminalpolitisch ist die Notwendigkeit des Nachverfolgens der Kommunikation in bestimmten Fällen unbestritten. Allerdings bereitet die konkrete Ausgestaltung der Maßnahme sowie die Wahrung der rechtsstaatlichen Grenzen Schwierigkeiten, was an § 100a StPO deutlich wird. In der derzeitigen Fassung stellt die Quellen-TKÜ eine Infiltrierung einer Hardware durch Malware dar. Der Staat nutzt also Lücken in der technischen Sicherheit eines Geräts aus. Dies stellt zwar einerseits einen massiven Grundrechtseingriff dar. Andererseits ist die Nachverfolgung dieser Kommunikation jedoch für eine effektive Strafverfolgung erforderlich. Die Praxis hat hier eine extrem sensible Abwägung durchzuführen.

1. Effizienz und Erforderlichkeit der Quellen-TKÜ

Von Seiten der Strafermittler wurde betont, dass die Quellen-TKÜ voraussichtlich keine Standardmaßnahme darstellen wird, sondern vielmehr einen Sonderfall. Die Umsetzung der Maßnahme gestaltet sich als schwierig, sie verursacht hohe Kosten und die Entdeckungsgefahr ist relativ hoch. Allein aus diesen Gründen wird die Maßnahme selbst bei rechtlicher Möglichkeit nur als Ausnahme eingesetzt werden. Des Weiteren sieht auch die StPO hohe Schranken für den Einsatz einer Quellen-TKÜ – wie z.B. den Richtervorbehalt – vor und bietet durch die Pflicht der nachträglichen Benachrichtigung entsprechende Kontrollmöglichkeiten. Eine Erforderlichkeit für solche, an die neuen Technologien angepasste, Eingriffsbefugnisse besteht nichtsdestotrotz insbesondere im Rahmen der komplexen Cyber-Ermittlungen. Zwar können hier grundsätzlich auch die altbewährten, klassischen Ermittlungsmaßnahmen Erfolg versprechen. Allerdings bedarf es aufgrund der Komplexität der Fälle einer Ausschöpfung sämtlicher Ermittlungsmethoden – im Einzelfall inklusive einer Quellen-TKÜ.

2. Backdoor-Lösung als Alternative zur Quellen-TKÜ

Als Alternative zur Quellen-TKÜ wurde aus den Reihen des Publikums eine sog. Backdoor-Lösung vorgeschlagen, bei der private Messenger-Dienste von staatlicher Seite dazu verpflichtet werden, TKÜ-Schnittstellen zur Überwachung durch Strafverfolgungsbehörden einzurichten. Von anderer Seite wurde neben einer generellen Befürwortung einer solchen Lösung auf das praktische Problem hingewiesen, dass die meisten Messenger-Dienste von ausländischen Firmen betrieben werden. Dies würde eventuell eine Verpflichtung der Dienste über multinationales Recht erfordern und einen Zugriff sämtlicher ausländischer Strafverfolgungsbehörden auf diese Sicherheitslücke mit sich bringen. Aus diesem Grund scheint die mit Genehmigungspflichten und Kontrollmechanismen ausgestattete Quellen-TKÜ nicht nur die praktikablere, sondern auch im Hinblick auf die rechtsstaatlichen Anforderungen bessere Lösung. Aus journalistischer Sicht ist im Rahmen einer Backdoor-Lösung die Gefahr zu beachten, dass eine bestehende Sicherheitslücke nicht nur von Strafverfolgungsbehörden, sondern auch von Hackern, Cyberbetrügern o.Ä. genutzt werden kann.

3. Umgang mit und Erlangung von Sicherheitslücken durch den Staat

In diesem Zusammenhang stellte sich die generelle Frage de staatlichen Umgangs mit solchen Sicherheitslücken. So wurde zu bedenken gegeben, dass der Staat im Falle des Auffindens einer Schwachstelle und der Nutzung ebendieser zu eigenen Zwecken gleichzeitig die Entscheidung trifft, das Bestehen der Sicherheitslücke nicht zu veröffentlichen. Damit nimmt der Staat in Kauf, dass auch andere Personen, z.B. Angreifer aus anderen Ländern, die gleiche Schwachstelle finden und nutzen können. Andere Länder sind in diesem Bereich fortschrittlicher: So existieren in den USA Standards, die regeln, welche Schwachstellen die Behörden veröffentlichen müssen und welche sie geheim halten dürfen. Diskutiert wurde ferner, ob diese Situation nicht zu einer innerpolitischen Schizophrenie führt. Ein Resort der inneren Sicherheit nutzt Schwachstellen für staatliche Zwecke und hält diese geheim, wohingegen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als dem Innenministerium unterstellte Behörde u.a. die Aufgabe obliegt, Bürger und deren IT-Sicherheit gegen Angriffe von außen zu stärken. Dem wurde entgegengehalten, dass es sich nicht um eine Schizophrenie handele, sondern lediglich um unterschiedliche Aufgaben des Staates, die in eine Waagschale geworfen und erfüllt werden müssen. Neben dem staatlichen Umgang mit Sicherheitslücken wurde die Frage aufgeworfen, wie der Staat überhaupt an solche Schwachstellen oder zu infiltrierende Malware gelangt. Sowohl ein direkter Kauf von Kriminellen auf einer Darknet-Plattform, als auch die Beauftragung eines Unternehmens mit einem solchen Kauf, würde ein kriminelles Netzwerk im Darknet fördern.

VI. Schlusswort und Fazit

Die abschließende Diskussionsrunde wurde durch ein Fazit des Veranstalters, *Prof. Safferling*, geschlossen: Den Bürgern wird im Hinblick auf sämtliche Eingriffsbefugnisse der Strafverfolgungsbehörden ein Grundvertrauen in die Funktionsweise des Rechtsstaats und dessen Kontrollmechanismen abverlangt. Gegenwärtig scheint ein solches Vertrauen der deutschen Bürger zu bestehen und die rechtsstaatlichen Anforderungen grundsätzlich gewahrt. Allerdings gibt es keine Garantie, dass der Rechtsstaat in seiner derzeitigen Verlässlichkeit bestehen bleibt. Aus diesem Grund bedarf es solcher Diskussionen, wie sie im Rahmen des ECCT 2018 geführt wurden, um die sich gegenüberstehenden Rechte der Bürger und die Pflichten des Staates auszutarieren. Vor diesem Hintergrund freuen sich *Prof. Safferling* und sein Team der International Criminal Law Research Unit über eine gelungene Tagung und blicken der Fortsetzung der Veranstaltungsreihe „Erlanger Cybercrime Tag“ im Jahr 2019 entgegen.